

VLSI IMPLEMENTATION OF METASTABILITY-BASED RANDOM NUMBER GENERATOR USING DELAY LADDERS

This application claims priority to Provisional Serial No. **60/454,837** filed **March 14, 2003**.

FIELD OF THE INVENTION

[0001] The invention relates to the phenomenon of metastability and the effect of metastability on semiconductors. More particularly, the present invention relates to the use of metastability in the field of random number generators by creating a random number generator that makes use of the phenomenon.

BACKGROUND ART

[0002] Latches and flip-flops are widely used in all types of electronic devices for counting, sampling, and storage of data. There are a number of different types of flip-flops named after their primary function, such as D-type flip-flops (data), J-K flip flops (J and K inputs), and R-S flip-flops (having R and S latches, standing for “reset” and “set”. D flip-flops are a clocked flip-flop having a one clock pulse delay for its output.

[0003] Conventional flip-flops, such as D-type, can be used to detect the logic state of an asynchronous digital signal with timing relative to the clock signal that is non-periodic.

[0004] For example, as shown in Fig. 1, a synchronous signal can be applied to the clock input (CLK) 105 of flip-flop 110, and a digital logic level of the asynchronous signal (the inverted output $\neg Q$ of the flip-flop) to be detected is directed to the D input. The output signal is subsequently inverted on the Q output. Afterward, the flip-flop changes state whenever the clock signal is changed, as long as the reset signal is tied permanently to ground.

[0005] When there are multiple systems linked together, and the systems operate at different frequencies, it has long been a problem of designers to attempt a synchronization of the systems. It is a well-known way to synchronize such systems by synchronizing one of the signals with a local clock generator, by the use of a flip-flop.

[0006] However, the above solution to the synchronization problem is not perfect, as the operating conditions of the flip-flops can be violated because hold times and setup times are not always consistent with the specifications (such as provided in the data sheets) of the flip

flops used. The violation of the flip-flops can cause them to go into an unstable (metastable) state that can affect the entire operation of the linked systems. Metastability can occur when both inputs to a latch are set at a logic high (11) and are subsequently set at a logic low (00).

[0007] Metastability can cause the latch outputs to oscillate unpredictably in a statistically known manner. While theoretically it is possible for the latch outputs to oscillate in a statistically known manner, in reality the latch will randomly shift and arrive at random output values. Such metastable values are then detected by other circuitry as different logic states.

[0008] In circuit design, it is necessary for an engineer to determine what influence metastable states may have in a particular design, and provide ways to overcome the bad effects that metastability could have on a circuit.

[0009] It has also been recognized that the output of a metastable flip-flop circuit is sufficiently random. Thus, the instant inventor submits that the randomness of the metastable flip-flop is sufficiently random to build a random number generator.

[0010] Fig. 1 also shows a diagram of a flip-flop 109 realized with cross connected NAND gates 108,110. This flip-flop receives its both data inputs from clock oscillator 105 through the clock input 106 of flip-flop 109, which shapes the clock signal to square-wave. The Q output 107 is connected to both of the NAND gates 108, 110 via delay devices, 112,114, respectively. If the two NAND gates 108,110 were truly identical, there would be no need for the delay devices to achieve the highest probability to get the flip-flop 109 to become metastable. However, the NAND gates will ordinarily differ somewhat, and their speed difference will influence the number of times metastability occurs in a time interval.

[0011] In VLS integrated circuits there have been attempts at tunable delay by using single tapped-buffer chains, but their implementation has not been practical. The delay resolution was too coarse for the dynamic fine tuning required to achieve the highest frequencies at which metastability occurs. Delays were also designed by the introduction of long wires of various lengths, which increased design expense and was found to be difficult to control using automatic layout tools and standard element libraries.

SUMMARY OF THE INVENTION

[0012] It is an object of the invention to provide a metastable random number generator using dual-tapped buffer ladders. Accordingly a random number generator of the present invention includes a clock, a series of dual-tapped-buffer ladders (also referred to as buffer-chains).

BRIEF DESCRIPTION OF THE DRAWING

[0013] Fig. 1 illustrates a conventional flip-flop with cross-connected Nand gates to be forced into a metastable state.

[0014] Fig. 2 is an illustration of one way that a dual-tapped buffer chain can be employed.

DETAILED EMBODIMENTS

[0015] Fig. 2 illustrates one way that a dual-tapped buffer chain can be arranged according to the present invention. It is understood by persons of ordinary skill in the art that the number of flip-flops shown was selected for explanatory purposes, and there can be different arrangements in terms of size and connectivity that fall within the spirit of the invention and the scope of the appended claims.

[0016] As shown in Fig. 2, a series of D-flip flops 205, 215, 225, 235, 245, 255 are connected to a top row of buffers, 210, 220, and 230, and to a bottom row of buffers, 240, 260, and 270. The top row buffers are identical, each with a delay = d_1 , whereas the bottom row buffers are also identical, each with a delay = d_2 .

[0017] The difference between the delay of the top and bottom row of buffers (d) is equal to:

$d = d_1 - d_2$, which can be a very small value. The cascading of the flip-flops via the buffers means that, for example, in the center row of flip-flops the signal delay between the D and L inputs is:

$d, -d, 2d, -2d, 3d, \dots$. With an extra flip-flop having its D and L inputs connected directly to the clock signal there can be any desired range of delays from $-n*d$ to $+n*d$, where n is the number of buffers in the delay ladder.

[0018] As also shown in Fig. 2, one flip-flop of each pair has its D and L inputs connected to corresponding taps at the outputs of the buffers, in this particular case wherein the D inputs of flip-flops 205, 225 and 245 are attached to the respective outputs of the top buffers 210, 220 and 230, and the L inputs of flip-flops 205, 225 and 245 are attached to the respective outputs of the bottom buffers 240, 260 and 270. The other flip-flop of each pair of flip-flops connects its D and L inputs reverse of the above, with the D input connected to the respective output of the bottom buffer, and the L input connected to the respective top buffer.

[0019] Although not shown in Fig. 2, the flip-flops 215...250 can have clock inputs (identified as the triangular shape in the flip-flop), that are connected to a signal of constant logic level 1, in order to keep the flip-flop always active. Whenever the signal changes at the data inputs D and L the states of flip-flops might also change, some of them could get metastable.

[0020] Each of the flip-flops has metastability detectors (275,280,285,290,295), which are circuits that describe whether the signal on their input is metastable. In order to generate metastability, the flip-flops can be clocked with an input that deliberately violates the setup or hold times (and possibly both) of the flip-flop to ensure meta-stable behavior. The metastable output will cause the flip-flop to be asynchronous when compared with the clock input. A well-known synchronizing circuit can be used to synchronize the meta-stable output of the flip-flop with the clock source. After this synchronization, the flip-flop output is compared by the metastability detector to an input wave to ascertain whether the input and the output of the flip-flop do not match, indicating that the flip flop is in a metastable state. U.S. patent application Philips disclosure 700720 filed March 6, 2000 is hereby incorporated by reference as background material regarding the provision of background information about the function of the metastability detectors.

[0021] The items illustrated in Fig. 2 are the front end of a random number generator. The last part of the circuit communicates with the metastability detectors to determine which circuit becomes the most metastable. The flip-flop having the highest count of metastability occurrences is chosen to generate random numbers from its output. This feature may be periodically revisited after a predetermined period of time, amount of numbers generated, etc. to ensure that there hasn't been a change in the flip-flop showing the most metastability.

[0022] Moreover, as the frequency of the metastability occurrences is changed, the counters/comparators can be reset (or this can be a periodic function) to find the flip-flop having the most current highest metastable count. In any case, the output of the selected flip-flop is used to generate random numbers.

[0023] There are many ways known in the art how these metastable events can be used to generate random numbers. Examples include the final logic value to which the metastable circuit resolves to, the time when the metastability occurs, the duration of the observed uncertain logic levels, etc.

[0024] Finally, it should be understood by persons of ordinary skill in the art that one particular use of the presently claimed invention could be a smart card, which may or may not be used for CD, DVD, solid state memory players, or perhaps encryption for making purchases, by having a random number generator according to the present invention embedded thereon. In addition, the metastability state flip-flops has the advantage of preventing one from trying to steal information from the smart card by measuring voltage fluctuations to obtain passwords, etc.

[0025] Thus, the two chains of buffers provide fine delay adjustments to reach metastable states. Since the two chains use buffers with slightly different delays, the delay difference between corresponding buffer outputs changes gradually along the ladder, providing high resolution in the relative delays of the two data signals. Thus, the most metastable flip-flop is ideally used to generate the random numbers in a best mode of the invention, although it is possible to use another of the flip-flops in the ladder if desired.

[0026] In addition, while D-type flip flops were used in this application, it is possible to use other types of flip-flops that can reach a metastable state by using data signals changing when violating their hold and setup times.